PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-088328
(43)Date of publication of application : 30.03.1999

---

(51)Int.Cl. H04L 12/24
H04L 12/26
G06F 13/00

---

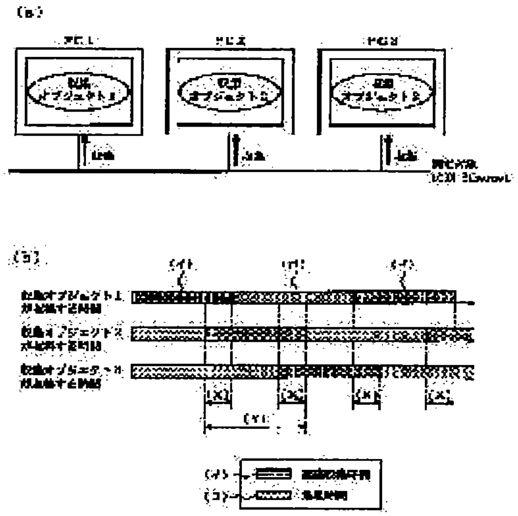
(21)Application number : 09-242338
(22)Date of filing : 08.09.1997

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : IKEGAMI SATOSHI
HAMADA MASAKI
MIKAMI HIROHIDE
KOMATSUBARA SHIGEYUKI

---

(54) TRAFFIC GATHERING AND ANALYZING SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a traffic gathering/analyzing system capable of gathering and analyzing traffic without omission in the transmission line of a wide band even at the time of using a traffic gathering/analyzing device with insufficient throughput.
SOLUTION: This system is provided with the plural traffic gathering/ analyzing devices (personal computers PC1-PC3) connected on the same network segment and respectively provided with traffic gathering/analyzing means (gathering objects 1-3) and a partial charge adjustment means (adjustment object or the like) for adjusting partial charges in the traffic gathering/analyzing means. By the partial charge adjustment means, the respective traffic gathering/ analyzing means are made to take the partial charges of the traffic on the network segment without the omission and gather and analyze it.



* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1]Two or more traffic collection and analysis apparatus in which it is connected on the same network segment and each possesses traffic collection and tools of analysis
A partial charge adjustment means which adjusts an assignment in said traffic collection and tools of analysis.
Are traffic collection and an analyzing system provided with the above, take and spill traffic on said network segment by said partial charge adjustment means to said traffic collection and tools of analysis, and it is made to assign that there is nothing, and is made to collect and analyze.

[Claim 2]In traffic collection and the analyzing system according to claim 1, said partial charge adjustment means, While each of said traffic collection and analysis apparatus decide beforehand that the attribute of a packet which should be collected and analyzed is taken and ****** does not occur, Traffic collection and an analyzing system being a means which detects and removes a packet which this overlaps when the same packets are being collected by two or more of said traffic collection and analysis apparatus.
[Claim 3]Traffic collection and an analyzing system characterized by the attribute of said packet being time for this packet to pass a network segment in traffic collection and the analyzing system according to claim 2.
[Claim 4]Traffic collection and an analyzing system characterized by the attribute of said packet being the information written in a header of this packet in traffic collection and the analyzing system according to claim 2.
[Claim 5]In traffic collection and the analyzing system according to claim 1, said partial charge adjustment means, While adjusting an assignment dynamically so that it may communicate and take mutually and ****** may not occur after each traffic collection and analysis apparatus start collection, Traffic collection and an analyzing system being a means which detects and removes a packet which this overlaps when the same packets are being collected by two or more of said traffic collection and analysis apparatus.
[Claim 6]In traffic collection and the analyzing system according to claim 5, dynamic adjustment of an assignment by said partial charge adjustment means, Frequency beforehand decided for every traffic collection and tools of analysis is made to share traffic processing, Traffic collection and an analyzing system shifting mutually an order of traffic treated by traffic collection and tools of analysis of this plurality when processing of the same traffic overlaps in two or more traffic collection and tools of analysis.

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]In this invention, load is especially distributed about the traffic collection and the analyzing system for performing traffic management in computer networks, such as the Internet.

Therefore, while making two or more low cheap machines of throughput cooperate and realizing high throughput, it takes and spills in a broadband transmission line, and is related with the traffic collection and the analyzing system it was made not to have **.

[0002]
[Description of the Prior Art]The packets which flow on a network are collected, and in traffic management of computer networks, such as the Internet, it is necessary to analyze them, to create various statistical datas or to save the contents of a packet depending on the case. As creation of a statistical data, there is creation of statistical information, such as the place of dispatch of a packet and a packet number according to mail arrival place, and there are preservation of the TCP/IP header of a packet, etc. as preservation of a packet, for example.
[0003]RMON (Remote network MONitoring) and RMON2 exists as a standard of the interface for accessing a collection item and the collected data in traffic collection. That to which the product for traffic collection and analysis in recent years was based on these standards occupies most. It is as follows when the traffic collection and analytical method based on RMON and RMON2 are classified.
The conventional method 1: How to collect with network equipment, such as a router and a hub (line concentrator).
The conventional method 2: How to collect by traffic collection and an analysis apparatus (probe).
Here with traffic collection and an analysis apparatus (probe). All the packets on a segment are investigated, it is analyzed and things, such as the dedicated hardware and the workstation which statistical information is created, or can save a packet so that it can analyze later, or PC (personal computer), are said.
[0004]
[Problem(s) to be Solved by the Invention]Generally, traffic collection and analysis are high processings of load, and the above-mentioned conventional methods 1 and 2 cannot necessarily say it as an effective method. Namely, since (1) traffic collection and analysis are high processings of load, It is difficult to make traffic collection processing that such loads are high perform to network equipment, such as a router and a hub (line concentrator), like the above-mentioned conventional method 1 in addition to original work (routing processing in the case of a router, etc.), in view of the throughput. It seems that the method of the conventional method 1 becomes increasingly effective less since it is expected that a network will be a broadband increasingly from now on.
(2) It seems that that the throughput of traffic collection and an analysis apparatus does not catch up occurs also by the method of the above-mentioned conventional method 2 using traffic collection and an analysis apparatus for exclusive use (probe). The fact that traffic collection and analysis processing will be a heavy load further in the future -- that the network has broadband-ized and traffic collection and an analytical item are various -- is cited as the reason.
[0005](3) Even if it has the ability for traffic collection and an analysis apparatus to perform traffic collection and analysis processing of a specific network, when using traffic collection and an analysis apparatus, there is a problem that great cost will start. As the reason, in order to require high processing of load, traffic collection and analysis, It is because it is necessary to use highly efficient traffic collection and analysis apparatus (probe) and each traffic collection and analysis apparatus (probe) become expensive in connection with it in a transmission line [broadband / backbone / (trunk-line data service network)]. In order to avoid it, when the traffic collection and the analysis apparatus (probe) whose throughput is not enough are used, collection and analysis processing can be performed to no packets, but it takes, ****** occurs, and the problem that it is not obtained generates exact statistics.
[0006](4) Further, on the Internet, in order to distribute generally without traffic's concentrating on a specified part, the installed number of traffic collection and an analysis apparatus increases. Therefore, the cost of each traffic collection and analysis apparatus poses a big problem. The purpose of this invention is to provide the traffic collection and the analyzing system which it takes and spills in a broadband transmission line, and can collect and analyze traffic that there is

nothing, even if it uses the traffic collection and the analysis apparatus for which throughput was insufficient, in order to solve these problems.

[0007]

[Means for Solving the Problem]To achieve the above objects, traffic collection and an analyzing system of this invention, Two or more traffic collection and analysis apparatus (for example, personal computer PC) in which it is connected on the same network segment and each possesses traffic collection and tools of analysis (a collection object, a collection process), Have a partial charge adjustment means which adjusts an assignment in said traffic collection and tools of analysis (a collection object, a collection process), and by a partial charge adjustment means. It is characterized by taking and spilling traffic on a network segment to each traffic collection and tools of analysis, making it assign that there is nothing, and making it collect and analyze.

[0008]While deciding beforehand that said partial charge adjustment means takes the attribute (time for a packet to pass a network segment, information written in a header of a packet) of a packet which each traffic collection and analysis apparatus should collect and analyze, and ****** does not generate it, When the same packets are being collected by two or more traffic collection and analysis apparatus, it is characterized by being what detects and removes a packet which this overlaps (examples 1 and 2: a partial charge adjustment means is equivalent to a function of a part of comparison object or collection object in this case).

[0009]While said partial charge adjustment means adjusts an assignment dynamically so that it may communicate and take mutually and ****** may not occur after each traffic collection and analysis apparatus start collection (even one side is adjusted with ******), When the same packets are being collected by two or more of said traffic collection and analysis apparatus, it is characterized by being what detects and removes a packet which this overlaps (example 3: a partial charge adjustment means is equivalent to an adjustment object in this case).

[0010]

[Embodiment of the Invention]The suitable embodiment of this invention has the following basic constitution.

** Install two or more traffic collection and analysis apparatus on the same segment of the network which conducts traffic collection and analysis.

** Operate the process (collection process) of conducting collection and analysis of traffic on each traffic collection and analysis apparatus.

** The packet which conducts collection and analysis is assigned to each collection process, and each collection process carries out collection and analysis for the packet which flows into a measuring object segment to it selectively according to the assignment.

** Total the traffic data collected and analyzed in each collection process.

[0011]The following method is used as assignment of the packet which each collection process in the above-mentioned ** collects and analyzes.

(a) How (how to opt for the assignment statically beforehand) to opt for assignment of the packet which each collection process collects and analyzes beforehand. There are a method of assigning beforehand the time zone which collects packets for every collection process as an example in this case, the method of assigning beforehand the attribute (it is a protocol etc. for example, it is written in a header) of the packet which should be collected for every collection process, etc.

(b) How (how to adjust an assignment dynamically working and to opt for it) to opt for an assignment by communicating mutually and adjusting between collection processes after each collection process starts. There is a method of opting for assignment of the packet which should be collected between collection processes dynamically referring to the arrival order foreword of the arriving packet as an example in this case.

[0012](division of roles and its effect) As a method of assigning the packet which should be collected in each collection process, ** mentioned above has ″the method of opting for the assignment beforehand″, and ″a method of adjusting and opting for an assignment.″

(a) The packet which should be collected in each collection process is beforehand opted for assignment, and method″ which opts for ″assignment beforehand is made to share a role.

According to this method, the load per traffic collection and analysis apparatus is reduced, and it becomes possible to collect and analyze all the traffic as a whole.
(in b) "method of adjusting and opting for an assignment", assignment of each collection process is dynamically changed during packet collection. Since the load of each traffic collection and analysis apparatus can be changed easily according to this method, scalability can be made high.
[0013](Take and spill) Since the role of each collection process is assigned so that picking ****** may not occur, if data is totaled from each collection process, the traffic data of the segment can be created.
[0014]Hereafter, the example of this invention is described in detail using a drawing. In this invention, methods of sharing the role of packet collection with each collection process include "the method of opting for the assignment beforehand", and "the method of adjusting and opting for an assignment." It is considered as "the method of opting for the assignment beforehand", and there are "method of opting for an assignment by the pass time of a packet", and "method of opting for an assignment with the header attribute of a packet." The case where "the method of adjusting and opting for an assignment" is used for the case where "the method of opting for an assignment with the header attribute of a packet" is hereafter used for the case where "the method of opting for an assignment by the pass time of a packet" is used as Example 1, as Example 2, as Example 3 is explained.
[0015](Example 1)
The explanatory view 1 of an example using "the method of opting for an assignment by the pass time of a packet" is a figure explaining the example which used "the method of opting for an assignment by the pass time of a packet." "The method of opting for an assignment by the pass time of a packet" is a method of opting for an assignment by assigning the time zone which synchronizes time between each traffic collection and analysis apparatus, and collects traffic in each collection process (collection object). That is, each collection process (collection object) is decided to perform collection and analysis processing only about the packet which passed the segment within the assigned time zone.
[0016]Drawing 1 (a) receives 100M Ethernet (registered trademark) (Ethernet of the specification which can be used by 100M bit per second), On three-set [of PCs] (personal computer), and personal computer PC1, PC2, and PC3, The example in the case of operating one collection object which communicates on a general-purpose distributed object plat form, and conducting traffic collection and analysis is shown, Between each personal computer PC, it is assumed that the time synchronization accuracy was guaranteed to be is performed using NTP (Network Time Protocol) etc. Suppose that the collection object 1 exists in personal computer PC1, the collection object 2 exists in personal computer PC2, and the collection object 3 exists in personal computer PC3.
[0017](Composition of a collection object) Drawing 2 is a block diagram showing the internal configuration of each collection objects 1-3. As for 20, in the figure, a primary buffer and 24 are memory measures a collection object and 22. The memory measure 24 may be, the database (DB) (Management InformationBase), i.e., MIB, of network management information which were standardized with the TCP/IP protocol. 21 shows the process treatment 1 which saves up a packet to the primary buffer 22, and 24 processes the packet saved up to the primary buffer 22, and shows the process treatment 2 which creates various statistical datas or saves the created various statistical datas and a packet at the memory measure 24.
[0018]Drawing 1 (b) is a figure showing the activity of each collection object 1-3 of the three personal computers PC1-PC3 along a time-axis top. In the figure, (b) shows "continuation collection time" and (**) shows "processing time." To the primary buffer 22, "continuation collection time" is the packet which passes the segment concerned time (time for the process treatment 1 to operate) to save up, and with "processing time." Various statistical datas are created from the collected packets, or time (time for the process treatment 2 to operate) to perform a packet and created preservation of a statistical data is expressed (refer to drawing 2).
[0019]Division of roles in this example is performed by assigning "continuation collection time" to each collection objects 1-3. In this case, if the synchronization between each continuation collection time is not exact, it will take at the time of a change and ****** will occur. In order to

prevent this, only the part of the accuracy of a synchronization needs to give a margin, i.e., a lap, between [of each collection object] continuation collection time.
[0020]The capacity of the primary buffer 22 of the collection object in this example is determined that it will fulfill the conditions of (1) type.
Accuracy x2 of the time synchronization by which the zone x guarantee of the capacity > measuring object transmission line of a primary buffer was done ... (1) type[0021]This reason is explained using continuation collection time (b) of drawing 1 (b), and processing time (**). In drawing 1, (X) expresses the lap time (grade of a synchronization) between each collection object, and (Y) expresses continuation collection time (b).These (X) and (Y) are determined as follows.
** Determine determining method (X) of (X) as follows.
(X)= accuracy of the guaranteed time synchronization ... the method (Y) of determining (2) type
** (Y) expresses 1 time of continuation collection time (b) of the collection object. This continuation collection time needs to fulfill the conditions of following the (3) type at least.
(Y) -- >(X)x2 ... (3) types -- here -- continuation collection time (Y) -- The zone of the capacity / measuring object transmission line of a continuation collection time = primary buffer ... it is expressed with (4) types. (3) It turns out that it is necessary to fulfill the conditions of a formula, and the conditions of (4) types to the above-mentioned (1) formula.
[0022]From the above-mentioned (1) formula, the capacity of a primary buffer can be determined in consideration of the zone of a measuring object transmission line, and the guaranteed accuracy of a time synchronization. For example, in the transmission line of 100M bps, when the synchronous accuracy for 10 ms is obtained. (X)= 10 ms ... (5) types (Y) >20ms ... in order to become (6) types and to fill (6) types, it turns out that what is necessary is just to prepare the primary buffer more than 2000K bits, i.e., a 250 K byte (= 2000/8) K bit.
[0023]The following thing becomes possible by taking the above composition.
** Within a time [to which each collection object was assigned] is continuously collectable (continuation collection).
** Take, when changing a role between each PC, and ****** does not occur.
[0024](The total method of data) How to ask for the set union of the information which each collection object collected is shown below.
(A) Save the packets collected by each collection object between parts for accuracy, i.e., time (X) currently overlapped and collected, of a synchronization.
(B) Compare the packet which it overlapped and were collected between (X)s between the collection objects currently collected, and ask for a duplicate packet.
(C) Overlap, conduct the same analysis as the collected packets to the packet currently collected, and save analytical data.
(D) Deduct the saved analytical data from the sum of data collected by the collection objects 1 and 2.
[0025]The comparison processing of the above (B), and analysis and storage processing of the packet which the above (C) overlaps and are collected have two kinds, the method of carrying out which it takes charge of by the object (it is henceforth called a comparison object) provided in its exclusive use, and the method which each collection object takes charge of. Hereafter, each is described.
** Provide the comparison object only for a method which provides a comparison object for exclusive use, and make this comparison object take charge of the comparison processing of the above (B), and analysis and storage processing of (C). Each collection object sends the packets collected between (X)s to a comparison object. In a comparison object, the data between the objects currently overlapped and collected is compared, a duplicate packet is computed, and analysis and storage processing of the above (C) are performed.
[0026]** Take charge of the comparison processing of the method above (B), and the analysis and storage processing of (C) with which each collection object compares only in one collection object of the two collection objects which overlap and are collecting packets. At this time, it overlaps and the collection object of another side of the two collection objects currently collected sends the packets collected during the (X) to above-mentioned one [which takes

charge of the comparison processing of (B), and analysis and storage processing of (C)] collection object. It is made, as for how to choose above-mentioned one [which takes charge of the comparison processing of (B), and analysis and storage processing of (C)] collection object, for load to distribute as much as possible. In the case of drawing 1 which consists of three collection objects, For example, comparison of the packets collected by the collection object 1, and the packets collected by the collection object 2 the collection object 1, The collection object 3 is made to perform comparison of the packet in which the collection object 2 collected comparison of the packets collected by the collection object 2, and the packets collected by the collection object 3 by the collection object 3, and the packets collected by the collection object 1, respectively.

[0027]Next, when overlapping and collecting between the collection object 1 and the collection object 2, how to ask for the packet number which passed the segment of the collection object is shown. Packet number p for which it asks is as follows.

p=x+y-z -- here, recovery of the packet number data which was collected by the packet number y:collection object 2 collected by x:collection object 1 and which was collected by carrying out packet number z:duplication, When the dedicated line for control can be prepared, it is satisfactory, but when it is impossible, the network which conducts traffic collection and analysis is used. In that case, in order to reduce the load to the network which conducts traffic collection and analysis, data is compressed and sent out.

[0028]Since composition which was mentioned above is adopted according to this example, it becomes possible to distribute load by two or more traffic collection and analysis apparatus, and to conduct traffic collection and analysis. Even if it is low PC of throughput in this example, it is available by shortening time to collect traffic and lengthening processing time.

[0029](Example 2)

Although it is possible to opt for the assignment of a collection object in a protocol, a source address, a destination address, etc. by explanation "method of opting for an assignment with the header attribute of a packet" of the example using "the method of opting for an assignment with the header attribute of a packet", It is considered [that load may incline greatly by generating of the load by a single user, and] on the Internet. For utilization, it is required to use the attribute which a bias does not generate, and the method of distributing load by ID identifier, a header checksum, etc., etc. are considered. In this case, determination of an assignment which a bias does not produce for load very much for a short time is needed.

[0030]In sharing a role using ID identifier, a header checksum, etc., unlike the case of the above-mentioned Example 1, it does not produce duplication in the packets collected by each collection object. this -- supposing in 1 bit of the last of ID identifier the collection object 2 collected the things of "0" and 1 bit of the last of ID identifier collects the things of "1", the collection object 1, Considering the example that it is lost that duplication arises in the packets collected by the collection objects 1 and 2, it is clear. Therefore, what is necessary is just to only take the sum of the data of each collection object, in calculating a statistic. Recovery of data uses the same method as Example 1.

[0031]According to this example, it becomes possible to distribute load by two or more general purpose computers, and to conduct collection and analysis of traffic. Even when low PC of throughput is used, it becomes available what the quantity of the collection packet of the PC is reduced for (the lower 2 figure of ID identifier collects the things of "00").

[0032](Example 3)

The explanatory view 3 of an example using "the method of adjusting and opting for an assignment" is a figure for describing the example of "the method of opting for an assignment based on an arrival order foreword" as an example of "the method of adjusting and opting for an assignment." "The method of opting for an assignment based on an arrival order foreword" is a way each collection object opts for an assignment dynamically using the arrival order foreword information on a segment. That is, each collection object is the method of collecting and analyzing in order the packet which arrives one after another. The arrival order foreword of the packet within the same segment can apply this method to the same thing like the shared media of a multiple access. The cooperation (adjustment) mechanism for not collecting the same

packets between each collection object in this method is indispensable.
[0033]Since order information is not included in the packet itself, the reason is because the packet which should be collected by each collection object is not known. For example, when two collection objects collect mutually in every other packet, suppose that the same packets were collected by both collection objects. An adjustment object is provided, these are supervised, and when it is detected that the same packets were collected by both collection objects, the method of directing to shift one packet collected to collection object of one of the two can be considered.
[0034]In drawing 3, to 100M Ethernet, traffic collection and analysis are conducted using two personal computers, and one collection object which communicates on a general-purpose distributed object plat form is operated on each personal computer. An adjustment object is operated with one of personal computers. The example of drawing 3 (a) shows the case where the collection object 1 and an adjustment object are operated on personal computer PC1, and it operates the collection object 2 on personal computer PC2.
[0035](Explanation of operation)
** Determine frequency n/m of the packet collected for every collection object according to the throughput of each PC before starting (n and m are natural numbers). Frequency n/m means collecting n packets of them correctly, when m packet arrives. The case of the frequency 2/5, i.e., n= 2, and m= 5 is made into an example, and this operation is shown in drawing 4. drawing 4 -- packet p (1), p (2), p (3), and ... p (5a+1), p (5a+2), and p (5a+3) -- in a collection object, when ... arrives. two fifths of the packets of them, i.e., p, (1), p (3), and ... it means collecting p (5a+1), p (5a+3), and ...
[0036]** Start each collection object simultaneously, and from arbitrary packets, it starts collection and collects n packets to m packet.
** After each collection object starts collection, an adjustment object investigates the packet which is collecting each collection objects.
** When two or more collection objects are collecting the same packets, calculate the adjustment method for each collection object, and take out directions to a collection object. In calculation of an adjustment method, in order to take and to lose ******, it is calculated how the packet which each collection object collects should be shifted.
[0037](Deciding method of frequency n/m of the packet to collect)
** Set n of the collection object on PC with the lowest throughput to 1 among PCs used for collection, and determine m suitable for capability.
** The collection object of other PCs determines n suitable for throughput using m determined by the above-mentioned **.
The number of PC is prepared so that the sum of n assigned to each collection object may become more than m.
[0038]This structure is concretely explained using drawing 3.
** Set the collection objects 1 and 2 to n= 1 and m= 2.
** Assume that two collection objects are collecting the same packet p (1), p (3), and p (5) by chance at the time of starting (refer to drawing 3 (b)).
** Investigate the packet in which the adjustment object is collecting each collection objects 1 and 2, trace that two collection objects are collecting the same packets, and issue directions so that one packet collected to the collection object 2 may be shifted.
** The collection object 1 continues collection in the same order as it or before (p (7), p (9), p (11), ...). On the other hand, as for a collection object, the one collection object 2 collects packet p (8) shifted one, p (10), and ... after it according to the directions to shift. It takes [subsequent], and spills and ** becomes thus, is not less by shifting every one packet collected by one collection object (refer to drawing 3 (c)).
[0039](Data total) In the case of this example, after adjustment is completed, the duplication of data is not produced. Therefore, what is necessary is just to only take the sum of the data of each collection object, in calculating a statistic. Recovery of data takes the same method as Example 1.
[0040]According to this example, it becomes possible to distribute load by two or more general

purpose computers, and to conduct collection and analysis of traffic by composition like the above. Also when load is distributed with low PC of throughput, it becomes available what collection service frequency of the packet of the PC is made small for (for example, ten PCs are prepared and each collects to ten packets [one]).

[0041]

[Effect of the Invention]According to this invention, by carrying out two or more set coordination operation, low PC (personal computer) of throughput also writes traffic collection and analysis as it is possible, and it can reduce the cost of traffic collection and analysis (reduction of cost). Since scalability is high, even when a zone increases, it can respond easily by increasing the number of a general purpose computer (the correspondence to a spread spectrum transmission way is possible).

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a figure showing the system configuration of Example 1 of this invention, and the example of each collection object of operation.

[Drawing 2]It is a figure showing the example of composition of the collection object of Example 1 of this invention.

[Drawing 3]It is a figure showing the system configuration of Example 3 of this invention, and the example of each object of operation.

[Drawing 4]In Example 3 of this invention, it is a figure showing the example of each collection object in case the collection service frequency of a packet is 2/5 of operation.

[Description of Notations]

20: A collection object, the 21:process treatment 1, 22:primary buffer, the 23:process treatment 2 and 24 : memory measure (MIB;Management Information Base)

[Translation done.]

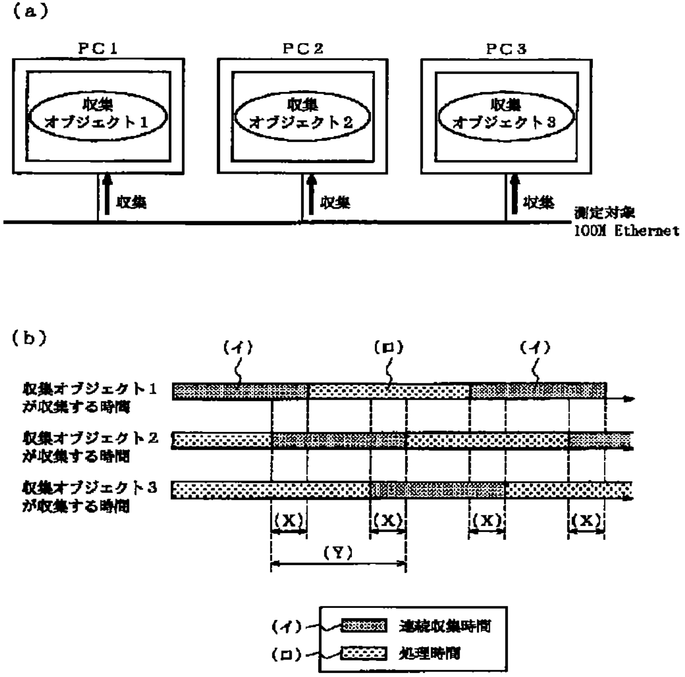
* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

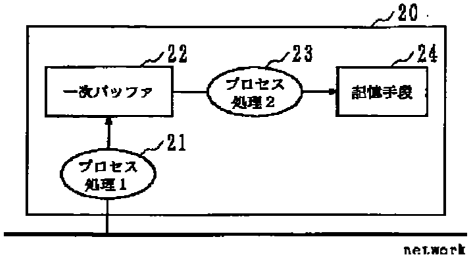
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

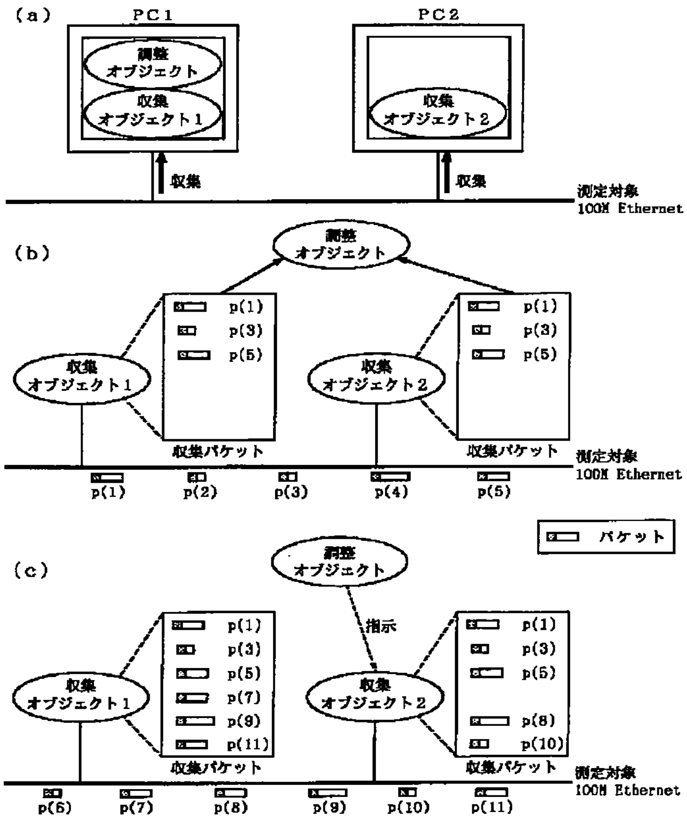
[Drawing 1]



[Drawing 2]

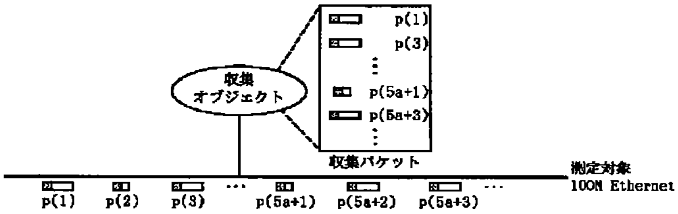


[Drawing 3]



[Drawing 4]

収集パケット頻度２／５の例



[Translation done.]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－88328

(43)公開日　平成11年(1999) 3月30日

(51)Int.Cl.⁶		識別記号	ＦＩ		
Ｈ０４Ｌ	12/24		Ｈ０４Ｌ	11/08	
	12/26		Ｇ０６Ｆ	13/00	３５１Ｎ
Ｇ０６Ｆ	13/00	３５１			

審査請求　未請求　請求項の数６　ＯＬ　（全 ８ 頁）

(21)出願番号　特願平9－242338

(22)出願日　平成９年(1997) ９月８日

特許法第30条第１項適用申請有り　平成９年３月12日～３月14日　社団法人情報処理学会主催の「情報処理学会　第54回（平成９年前期）全国大会」において文書をもって発表

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　池上　聡
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　浜田　雅樹
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　三上　博英
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(74)代理人　弁理士　磯村　雅俊　（外１名）

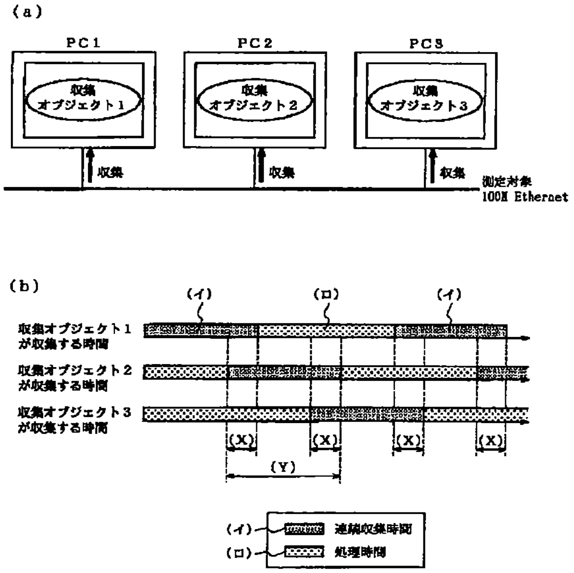
最終頁に続く

(54)【発明の名称】　トラフィック収集・分析システム

(57)【要約】

【課題】　処理能力の不足したトラフィック収集・分析装置を用いても、広帯域な伝送路で取りこぼしなくトラフィックを収集・分析することが可能なトラフィック収集・分析システムを提供すること。

【解決手段】　同一のネットワークセグメント上に接続され、各々がトラフィック収集・分析手段（収集オブジェクト１～３）を具備する複数のトラフィック収集・分析装置（パーソナルコンピュータＰＣ１～３）と、トラフィック収集・分析手段における分担を調整する分担調整手段（調整オブジェクトなど）とを有し、該分担調整手段により、ネットワークセグメント上のトラフィックを、各トラフィック収集・分析手段に取りこぼしなく分担させて収集・分析させる。



【特許請求の範囲】

【請求項１】　同一のネットワークセグメント上に接続され、各々がトラフィック収集・分析手段を具備する複数のトラフィック収集・分析装置と、前記トラフィック収集・分析手段における分担を調整する分担調整手段とを有するコンピュータネットワークのトラフィック収集・分析システムであって、

前記分担調整手段により、前記ネットワークセグメント上のトラフィックを、前記トラフィック収集・分析手段に取りこぼしなく分担させて収集・分析させることを特徴とするトラフィック収集・分析システム。

【請求項２】　請求項１記載のトラフィック収集・分析システムにおいて、

前記分担調整手段は、前記各トラフィック収集・分析装置が収集・分析すべきパケットの属性を取りこぼしが発生しないように予め決めておくとともに、前記複数のトラフィック収集・分析装置で同一のパケットを収集している場合に、該重複しているパケットを検出して取り除く手段であることを特徴とするトラフィック収集・分析システム。

【請求項３】　請求項２記載のトラフィック収集・分析システムにおいて、

前記パケットの属性は、該パケットがネットワークセグメントを通過する時間であることを特徴とするトラフィック収集・分析システム。

【請求項４】　請求項２記載のトラフィック収集・分析システムにおいて、

前記パケットの属性は、該パケットのヘッダに書き込まれた情報であることを特徴とするトラフィック収集・分析システム。

【請求項５】　請求項１記載のトラフィック収集・分析システムにおいて、

前記分担調整手段は、各トラフィック収集・分析装置が収集を開始した後、相互に通信して取りこぼしが発生しないように分担を動的に調整するとともに、前記複数のトラフィック収集・分析装置で同一のパケットを収集している場合には、該重複しているパケットを検出して取り除く手段であることを特徴とするトラフィック収集・分析システム。

【請求項６】　請求項５記載のトラフィック収集・分析システムにおいて、前記分担調整手段による分担の動的な調整は、各トラフィック収集・分析手段ごとに予め決められた頻度でトラフィック処理を分担させ、同一のトラフィックの処理が複数のトラフィック収集・分析手段で重複した場合に、該複数のトラフィック収集・分析手段で扱うトラフィックの順序を互いにずらすようにしたことを特徴とするトラフィック収集・分析システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、インターネットなどのコンピュータネットワークにおけるトラフィック管理を行うためのトラフィック収集・分析システムに関し、特に、負荷を分散させることにより処理能力の低い安価なマシンを複数協調させて高い処理能力を実現するとともに、広帯域な伝送路で取りこぼしがないようにしたトラフィック収集・分析システムに関する。

【０００２】

【従来の技術】インターネットなどのコンピュータネットワークのトラフィック管理においては、ネットワーク上を流れるパケットを収集し、それらを分析して様々な統計データを作成したり、場合によってはパケット内容を保存しておく必要がある。統計データの作成としては、例えば、パケットの発信地、着信地別パケット数などの統計情報の作成があり、パケットの保存としては、パケットのＴＣＰ／ＩＰヘッダの保存などがある。

【０００３】トラフィック収集における、収集項目や収集されたデータにアクセスするためのインタフェースの標準として、ＲＭＯＮ（Ｒemote network ＭＯＮitoring）、ＲＭＯＮ２が存在する。近年のトラフィック収集・分析のための製品は、これらの標準に準拠したものが大半を占める。ＲＭＯＮ、ＲＭＯＮ２に準拠したトラフィック収集・分析方法を分類すると以下のようになる。

従来方法１：ルータやハブ（集線装置）などのネットワーク機器で収集する方法。

従来方法２：トラフィック収集・分析装置（プローブ）で収集する方法。

ここで、トラフィック収集・分析装置（プローブ）とは、セグメント上の全てのパケットを調査し、それを分析して統計情報を作成したり、後から分析できるようにパケットを保存しておくことが可能な、専用ハードウエア，ワークステーション，またはＰＣ（パーソナルコンピュータ）などのことをいう。

【０００４】

【発明が解決しようとする課題】一般に、トラフィック収集・分析は負荷の高い処理であり、上記従来方法１および２は必ずしも有効な方法とはいえない。すなわち、

（１）トラフィック収集・分析は負荷の高い処理であるため、上記従来方法１のように、ルータやハブ（集線装置）などのネットワーク機器に、本来の仕事（ルータの場合におけるルーチング処理など）に加えてこれらの負荷の高いトラフィック収集処理を行わせることはその処理能力からみて難しい。また、今後、ネットワークはますます広帯域になっていくことが予想されるため、従来方法１の方法はますます有効でなくなると思われる。

（２）専用のトラフィック収集・分析装置（プローブ）を用いる上記従来方法２の方法によっても、トラフィック収集・分析装置の処理能力が追いつかないことが発生すると思われる。その理由としては、ネットワークが広帯域化していること、トラフィック収集・分析項目が多岐にわたること、など、将来的にトラフィック収集・分

析処理は一層高負荷となることが挙げられる。

【０００５】（３）また、もしトラフィック収集・分析装置が特定ネットワークのトラフィック収集・分析処理を行う能力があったとしても、トラフィック収集・分析装置を用いる場合には多大のコストがかかってしまうという問題がある。その理由としては、トラフィック収集・分析は負荷の高い処理を要求するために、バックボーン（基幹ネットワーク）などの広帯域な伝送路では高性能なトラフィック収集・分析装置（プローブ）を用いる必要があり、それに伴い、個々のトラフィック収集・分析装置（プローブ）が高価になってしまうためである。それを回避するために処理能力が十分でないトラフィック収集・分析装置（プローブ）を用いた場合、全てのパケットに対して収集・分析処理を行うことができず、取りこぼしが発生し、正確な統計値などは得られないという問題が発生する。

【０００６】（４）さらに、インターネットでは、一般に、トラフィックが特定箇所に集中しないで分散するため、トラフィック収集・分析装置の設置数が多くなる。そのため、個々のトラフィック収集・分析装置のコストが大きな問題となる。本発明の目的は、これらの問題を解決するため、処理能力の不足したトラフィック収集・分析装置を用いても、広帯域な伝送路で取りこぼしなくトラフィックを収集・分析することが可能なトラフィック収集・分析システムを提供することである。

【０００７】

【課題を解決するための手段】上記目的を達成するために、本発明のトラフィック収集・分析システムは、同一のネットワークセグメント上に接続され、各々がトラフィック収集・分析手段（収集オブジェクト，収集プロセス）を具備する複数のトラフィック収集・分析装置（例えば、パーソナルコンピュータＰＣ）と、前記トラフィック収集・分析手段（収集オブジェクト，収集プロセス）における分担を調整する分担調整手段とを有し、分担調整手段により、ネットワークセグメント上のトラフィックを、各トラフィック収集・分析手段に取りこぼしなく分担させて収集・分析させることを特徴としている。

【０００８】また、前記分担調整手段は、各トラフィック収集・分析装置が収集・分析すべきパケットの属性（パケットがネットワークセグメントを通過する時間，パケットのヘッダに書き込まれた情報）を取りこぼしが発生しないように予め決めておくとともに、複数のトラフィック収集・分析装置で同一のパケットを収集している場合に、該重複しているパケットを検出して取り除くものであることを特徴としている（実施例１，２：この場合、分担調整手段は比較オブジェクトまたは収集オブジェクトの一部の機能に相当）。

【０００９】また、前記分担調整手段は、各トラフィック収集・分析装置が収集を開始した後、相互に通信して取りこぼしが発生しないように分担を動的に調整（一方をすらすことによって調整）するとともに、前記複数のトラフィック収集・分析装置で同一のパケットを収集している場合には、該重複しているパケットを検出して取り除くものであることを特徴としている（実施例３：この場合、分担調整手段は調整オブジェクトに相当）。

【００１０】

【発明の実施の形態】本発明の好適な実施の形態は次のような基本構成を有する。

①複数のトラフィック収集・分析装置をトラフィック収集・分析を行うネットワークの同一セグメント上に設置する。

②各トラフィック収集・分析装置上でトラフィックの収集・分析を行うプロセス（収集プロセス）を動作させる。

③各収集プロセスには、収集・分析を行うパケットが割り当てられ、各収集プロセスは、その割り当てに従って、測定対象セグメントに流れるパケットを選択的に収集・分析を行う。

④各収集プロセスで収集・分析したトラフィックデータを集計する。

【００１１】上記③における、各収集プロセスが収集・分析するパケットの割り当てとしては次の方法が用いられる。

（ａ）各収集プロセスが収集・分析するパケットの割り当てを予め決めておく方法（分担を予め静的に決めておく方法）。この場合の例として、収集プロセスごとにパケットを収集する時間帯を予め割り当てておく方法、収集プロセスごとに収集すべきパケットの属性（ヘッダに書き込まれる例えばプロトコルなど）を予め割り当てておく方法などがある。

（ｂ）各収集プロセスが起動してから、収集プロセス間で互いに通信して調整することで分担を決める方法（分担を動作中に動的に調整して決める方法）。この場合の例として、到着するパケットの到着順序を参照しながら収集プロセス間で収集すべきパケットの割り当てを動的に決める方法がある。

【００１２】（役割分担とその効果について）各収集プロセスに収集すべきパケットを割り当てる方法としては、上述したよに「分担を予め決めておく方法」と「調整して分担を決める方法」とがある。

（ａ）「分担を予め決めておく方法」では、各収集プロセスに収集すべきパケットを割り当てを予め決めておき、役割を分担させる。本方法によれば、トラフィック収集・分析装置一台当たりの負荷を減らし、全体として、全てのトラフィックを収集・分析することが可能になる。

（ｂ）「調整して分担を決める方法」では、各収集プロセスの割り当てをパケット収集中に動的に変更する。本方法によれば、簡単に各トラフィック収集・分析装置の

負荷を変更することができるので、スケーラビリティを高くすることができる。

【００１３】（取りこぼしについて）取りこぼしが発生しないように各収集プロセスの役割を割り当てるので、各収集プロセスからデータを集計すれば、そのセグメントのトラフィックデータが作成できる。

【００１４】以下、本発明の実施例を図面を用いて詳細に説明する。本発明において、パケット収集の役割を各収集プロセスに分担する方法として、「分担を予め決めておく方法」と「調整して分担を決める方法」がある。また、「分担を予め決めておく方法」として、「パケットの通過時間で分担を決める方法」と「パケットのヘッダ属性によって分担を決める方法」がある。以下、実施例１として「パケットの通過時間で分担を決める方法」を用いた場合を、実施例２として「パケットのヘッダ属性によって分担を決める方法」を用いた場合を、実施例３として「調整して分担を決める方法」を用いた場合を説明する。

【００１５】（実施例１）
「パケットの通過時間で分担を決める方法」を用いた実施例の説明
図１は、「パケットの通過時間で分担を決める方法」を用いた実施例を説明する図である。「パケットの通過時間で分担を決める方法」とは、各トラフィック収集・分析装置間で時間を同期させ、それぞれの収集プロセス（収集オブジェクト）にトラフィックを収集する時間帯を割り当てることで分担を決める方法である。つまり、各収集プロセス（収集オブジェクト）は、割り当てられた時間帯内にそのセグメントを通過したパケットに関してのみ収集・分析処理を行うように決められる。

【００１６】図１（ａ）は、１００Ｍ Ｅｔｈｅｒｎｅｔ（登録商標）（１００Ｍビット／秒で利用できる仕様のイーサネット）に対して、３台のＰＣ（パーソナルコンピュータ）すなわちパーソナルコンピュータＰＣ１，ＰＣ２，ＰＣ３上で、汎用分散オブジェクトプラットフォーム上で通信を行う収集オブジェクトを一つ動作させてトラフィック収集・分析を行う場合の例を示しており、各パーソナルコンピュータＰＣ間ではＮＴＰ（Network Time Protocol）などを用いて、精度が保証された時間同期を行っているものとする。パーソナルコンピュータＰＣ１に収集オブジェクト１が、パーソナルコンピュータＰＣ２に収集オブジェクト２が、パーソナルコンピュータＰＣ３に収集オブジェクト３が存在するとする。

【００１７】（収集オブジェクトの構成）図２は、各収集オブジェクト１～３の内部構成を示すブロック図である。同図において、２０は収集オブジェクト、２２は一次バッファ、２４は記憶手段である。記憶手段２４は、ＴＣＰ／ＩＰプロトコルで標準化されたネットワーク管理情報のデータベース（ＤＢ）すなわちＭＩＢ（Management InformationBase）であってよい。２１は、パケットを一次バッファ２２に溜め込むプロセス処理１を示し、２４は、一次バッファ２２に溜め込んだパケットを処理して各種統計データを作成したり、作成した各種統計データやパケットを記憶手段２４に保存したりするプロセス処理２を示している。

【００１８】図１（ｂ）は、３つのパーソナルコンピュータＰＣ１～ＰＣ３のそれぞれの収集オブジェクト１～３の動作内容を時間軸上に沿って示した図である。同図において、（イ）は「連続収集時間」、（ロ）は「処理時間」を示している。「連続収集時間」とは、当該セグメントを通過するパケットを一次バッファ２２に溜め込む時間（プロセス処理１が動作する時間）であり、「処理時間」とは、収集したパケットから各種統計データを作成したり、パケットや作成した統計データの保存を行う時間（プロセス処理２が動作する時間）を表している（図２参照）。

【００１９】本実施例における役割分担は、各収集オブジェクト１～３に「連続収集時間」を割り当てることによって行われる。この場合、各連続収集時間間の同期が正確でないと、切り換え時に取りこぼしが発生してしまう。これを防ぐために、同期の精度の分だけ、各収集オブジェクトの連続収集時間相互間に余裕すなわち重なりを持たせる必要がある。

【００２０】本実施例における収集オブジェクトの一次バッファ２２の容量は（１）式の条件を満たすように決定される。

一次バッファの容量＞測定対象伝送路の帯域×保証された時間同期の精度×２
・・・（１）式

【００２１】この理由を、図１（ｂ）の連続収集時間（イ）、処理時間（ロ）を用いて説明する。図１中において、（Ｘ）は各収集オブジェクト間の重なり時間（同期の程度）を表し、（Ｙ）は連続収集時間（イ）を表している。これら（Ｘ）および（Ｙ）は以下のように決定される。

①（Ｘ）の決定法
（Ｘ）は以下のように決定する。

（Ｘ）＝保証された時間同期の精度
・・・（２）式

②（Ｙ）の決定法
（Ｙ）は収集オブジェクトの一回の連続収集時間（イ）を表している。この連続収集時間は少なくとも下記（３）式の条件を満たす必要がある。

（Ｙ）＞（Ｘ）×２
・・・（３）式

ここで、連続収集時間（Ｙ）は、

連続収集時間＝一次バッファの容量／測定対象伝送路の帯域・・・（４）式

で表される。（３）式の条件および（４）式から上記（１）式の条件を満たす必要があることがわかる。

【００２２】上記（１）式より、測定対象伝送路の帯域および保証された時間同期の精度を考慮して一次バッファの容量を決定することができる。例えば、１００Ｍｂｐｓの伝送路において、１０ｍｓの同期精度が得られた場合には、

（Ｘ）＝１０ｍｓ　・・・（５）式

（Ｙ）＞２０ｍｓ　・・・（６）式

となり、（６）式を満たすためには、２０００Ｋビットすなわち２５０Ｋバイト（＝２０００／８）Ｋビット以上の一次バッファを用意すればよいことがわかる。

【００２３】以上のような構成をとることによって次のことが可能になる。

①各収集オブジェクトが割り当てられた時間内は連続して収集（連続収集）できる。

②各ＰＣ間で役割を切り替える時に取りこぼしが発生しない。

【００２４】（データの集計方法）それぞれの収集オブジェクトが収集した情報の和集合を求める方法を以下に示す。

（Ａ）それぞれの収集オブジェクトで同期の精度分すなわち重複して収集している時間（Ｘ）の間に収集したパケットを保存しておく。

（Ｂ）重複して収集している収集オブジェクト間で（Ｘ）の間に収集したパケットを比較し、重複しているパケットを求める。

（Ｃ）重複して収集しているパケットに対し、収集したパケットと同様の分析を行い、分析データを保存する。

（Ｄ）その保存した分析データを収集オブジェクト１および２で収集したデータの和から差し引く。

【００２５】上記（Ｂ）の比較処理、および上記（Ｃ）の重複して収集しているパケットの分析・保存処理は、それ専用に設けられたオブジェクト（以降、比較オブジェクトと呼ぶ）によって担当するする方法と、各収集オブジェクトが担当する方法の二種類がある。以下、それぞれについて述べる。

①専用の比較オブジェクトを設ける方法

専用の比較オブジェクトを設け、上記（Ｂ）の比較処理および（Ｃ）の分析・保存処理を該比較オブジェクトに担当させる。各収集オブジェクトは、（Ｘ）の間に収集したパケットを比較オブジェクトに送る。比較オブジェクトでは、重複して収集しているオブジェクト間のデータを比較し、そして、重複しているパケットを算出して、上記（Ｃ）の分析・保存処理を行う。

【００２６】②各収集オブジェクトが比較を行う方法

上記（Ｂ）の比較処理および（Ｃ）の分析・保存処理は、パケットを重複して収集している２つの収集オブジェクトのうちの一方の収集オブジェクトだけで担当する。このとき、重複して収集している２つの収集オブジェクトのうちの他方の収集オブジェクトは、（Ｘ）の期間に収集したパケットを、（Ｂ）の比較処理および（Ｃ）の分析・保存処理を担当する上記一方の収集オブジェクトに送る。（Ｂ）の比較処理および（Ｃ）の分析・保存処理を担当する上記一方の収集オブジェクトの選び方は負荷ができるだけ分散するようにする。３つの収集オブジェクトからなる図１の場合では、例えば、収集オブジェクト１で収集したパケットと収集オブジェクト２で収集したパケットの比較は収集オブジェクト１が、収集オブジェクト２で収集したパケットと収集オブジェクト３で収集したパケットの比較は収集オブジェクト２が、収集オブジェクト３で収集したパケットと収集オブジェクト１で収集したパケットの比較は収集オブジェクト３がそれぞれ行うようにする。

【００２７】次に、収集オブジェクト１と収集オブジェクト２の間で重複して収集している場合に、収集対象のセグメントを通過したパケット数の求め方を示す。求めるパケット数ｐは以下のようになる。

ｐ＝ｘ＋ｙ－ｚ

ここで、ｘ：収集オブジェクト１で収集されたパケット数

ｙ：収集オブジェクト２で収集されたパケット数

ｚ：重複して収集されたパケット数

データの回収は、制御用の専用回線を用意できる場合は問題ないが、それが不可能な場合は、トラフィック収集・分析を行うネットワークを利用する。その際は、トラフィック収集・分析を行うネットワークに対する負荷を軽減するためにデータを圧縮して送出する。

【００２８】本実施例によると、上述したような構成を採用しているため、複数のトラフィック収集・分析装置で負荷を分散させてトラフィック収集・分析を行うことが可能になる。また、本実施例では、処理能力の低いＰＣであっても、トラフィックを収集する時間を短くし、処理時間を長くすることで利用可能である。

【００２９】（実施例２）

「パケットのヘッダ属性で分担を決める方法」を用いた実施例の説明

「パケットのヘッダ属性で分担を決める方法」では、プロトコル，ソースアドレス，ディスティネーションアドレスなどで収集オブジェクトの分担を決めることが考えられるが、インターネットでは単一のユーザによる負荷の発生により負荷が大きく偏る場合があると思われる。実用化のためには偏りが発生しない属性を用いることが必要であり、ＩＤ識別子，ヘッダチェックサムなどにより負荷を分散させる方法なども考えられる。この場合、

ごく短時間で負荷に偏りが生じないような分担の決定が必要となる。

【００３０】ＩＤ識別子，ヘッダチェックサムなどを用いて役割を分担する場合には、上記実施例１の場合とは異なり、各収集オブジェクトで収集したパケットに重複を生じることはない。このことは、収集オブジェクト１がＩＤ識別子の最後の１ビットが「０」のものを、収集オブジェクト２がＩＤ識別子の最後の１ビットが「１」のものを収集したとすると、収集オブジェクト１と２で収集したパケットに重複が生じることがなくなる、という例を考えれば明らかである。従って、統計値を求める場合には、単に各収集オブジェクトのデータの和をとるだけでよい。また、データの回収は、実施例１と同様の方法を用いる。

【００３１】本実施例によると、複数の汎用コンピュータで負荷を分散させてトラフィックの収集・分析を行うことが可能になる。また、処理能力の低いＰＣを用いた場合でも、そのＰＣの収集パケットの量を減らす（ＩＤ識別子の下２桁が「００」のものを収集）ことで利用可能となる。

【００３２】（実施例３）
「調整して分担を決める方法」を用いた実施例の説明
図３は、「調整して分担を決める方法」の一例として、「到着順序に基づいて分担を決める方法」の実施例を説明するための図である。「到着順序に基づいて分担を決める方法」とは、各収集オブジェクトがセグメント上での到着順序情報を用いて動的に分担を決める方法である。つまり、各収集オブジェクトが次々に到着するパケットを順番に収集・分析する方法である。この方法は、マルチプルアクセスのシェアードメディアのように、同一セグメント内でのパケットの到着順序が同一であるものに対して適用することができる。この方法では、各収集オブジェクト間で同一のパケットを収集しないための協調（調整）機構が不可欠である。

【００３３】その理由は、パケット自身には順序情報が含まれていないので、それぞれの収集オブジェクトで収集すべきパケットがわからないためである。例えば、２つの収集オブジェクトが互いに１パケットおきに収集した場合に、両方の収集オブジェクトで同一のパケットを収集したとする。調整オブジェクトを設けてこれらを監視し、同一のパケットが両方の収集オブジェクトで収集されたことが検知された場合には、片方の収集オブジェクトに対して収集するパケットを１つずらすように指示するなどの方法が考えられる。

【００３４】図３では、１００Ｍ Ｅthernetに対して、２台のパーソナルコンピュータを用いてトラフィック収集・分析を行っており、各パーソナルコンピュータ上では、汎用分散オブジェクトプラットフォーム上で通信を行う収集オブジェクトを一つ動作させる。また、いずれか一方のパーソナルコンピュータで調整オブジェクトを動作させる。図３（ａ）の例は、パーソナルコンピュータＰＣ１上で収集オブジェクト１と調整オブジェクトを、パーソナルコンピュータＰＣ２上で収集オブジェクト２を動作させた場合を示している。

【００３５】（動作説明）
①起動前に各ＰＣの処理能力に応じて、各収集オブジェクト毎に収集するパケットの頻度ｎ／ｍを決定する（ｎ，ｍは自然数）。頻度ｎ／ｍは、ｍパケットが到着したとき正確にそのうちのｎパケットを収集することを意味する。この動作を頻度２／５、すなわち、ｎ＝２、ｍ＝５の場合を例にして図４に示す。図４では、パケットｐ（１），ｐ（２），ｐ（３）、・・・ｐ（５ａ＋１）、ｐ（５ａ＋２）、ｐ（５ａ＋３）・・・が到着した場合、収集オブジェクトでは、そのうちの２／５のパケット、すなわち、ｐ（１）、ｐ（３）、・・・ｐ（５ａ＋１）、ｐ（５ａ＋３）、・・・を収集することを表している。

【００３６】②各収集オブジェクトは、同時に起動し、任意のパケットより収集を開始し、ｍパケットにｎパケットを収集する。
③各収集オブジェクトが収集を開始した後、調整オブジェクトが各収集オブジェクトの収集しているパケットを調査する。
④複数の収集オブジェクトが同一のパケットを収集している場合には、各収集オブジェクトに対する調整方法を計算し、収集オブジェクトに指示を出す。調整方法の計算では、取りこぼしをなくすために、各収集オブジェクトの収集するパケットをどのようにずらせばよいかを計算する。

【００３７】（収集するパケットの頻度ｎ／ｍの決定方法）
①収集に用いるＰＣのうち、最も処理能力の低いＰＣ上の収集オブジェクトのｎを１とし、能力相応のｍを決定する。
②他のＰＣの収集オブジェクトは、上記①で決定されたｍを用いて、処理能力相応のｎを決定する。
また、各収集オブジェクトに割り当てたｎの和がm以上となるようにＰＣの台数を用意する。

【００３８】この仕組みを、図３を用いて具体的に説明する。
①収集オブジェクト１，２ともに、ｎ＝１，ｍ＝２とする。
②起動時は２つの収集オブジェクトがたまたま同一のパケットｐ（１），ｐ（３），ｐ（５）を収集しているとする（図３（ｂ）参照）。
③調整オブジェクトが各収集オブジェクト１，２の収集しているパケットを調査し、２つの収集オブジェクトが同一のパケットを収集していることをつきとめ、収集オブジェクト２に収集するパケットを一つずらすように指示を出す。

④収集オブジェクト１はそれ以前と同様の順序で収集を続ける（ｐ（７），ｐ（９），ｐ（１１），・・・）。一方、収集オブジェクトは、収集オブジェクト２は一つずらす指示に従い、それ以降、一つずれたパケットｐ（８），ｐ（１０），・・・）を収集する。このように一方の収集オブジェクトで収集するパケットを一つずつずらすことによって、以降の取りこぼしがなくなる（図３（ｃ）参照）。

【００３９】（データ集計）本実施例の場合、調整が完了した後はデータの重複は生じない。従って、統計値を求める場合には、単に各収集オブジェクトのデータの和を取るだけでよい。また、データの回収は実施例１と同様の方法を取る。

【００４０】本実施例によると、上記の如き構成により、複数の汎用コンピュータで負荷を分散させてトラフィックの収集・分析を行うことが可能になる。また、処理能力の低いＰＣで負荷を分散させた場合にも、そのＰＣのパケットの収集頻度を小さくする（例えば、ＰＣを１０台用意し、それぞれが１０パケットに１つ収集する）ことで利用可能となる。

【００４１】【発明の効果】本発明によれば、処理能力の低いＰＣ（パーソナルコンピュータ）でも複数台協調動作させることで、トラフィック収集・分析を可能としたため、トラフィック収集・分析のコストが軽減できる（コストの削減）。また、スケーラビリティが高いため、帯域が増えた場合でも汎用コンピュータの台数を増やすことで簡単に対応できる（広帯域伝送路へ対応可能）。

【図面の簡単な説明】

【図１】本発明の実施例１のシステム構成、および、各収集オブジェクトの動作例を示す図である。

【図２】本発明の実施例１の収集オブジェクトの構成例を示す図である。

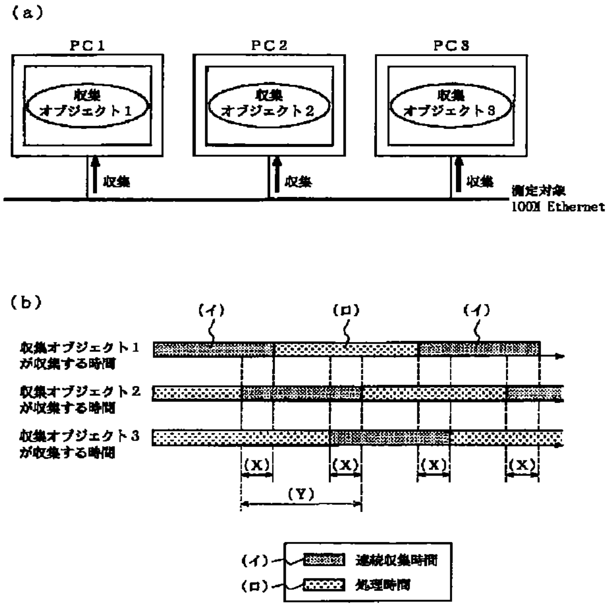
【図３】本発明の実施例３のシステム構成、および、各オブジェクトの動作例を示す図である。

【図４】本発明の実施例３において、パケットの収集頻度が２／５のときの各収集オブジェクトの動作例を示す図である。

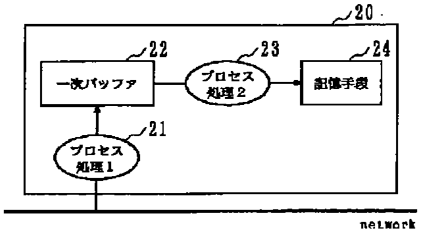
【符号の説明】

２０：収集オブジェクト、２１：プロセス処理１、２２：一次バッファ、２３：プロセス処理２、２４：記憶手段（ＭＩＢ；Management Ｉnformation Ｂase）

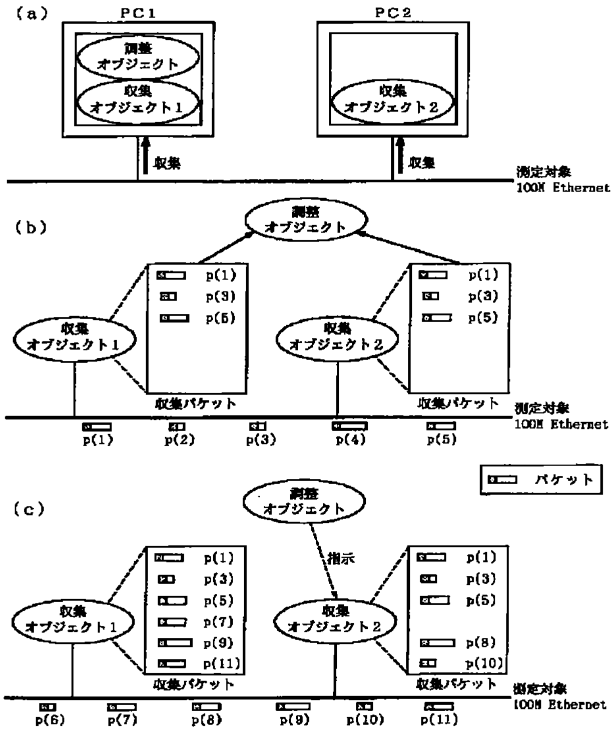
【図１】



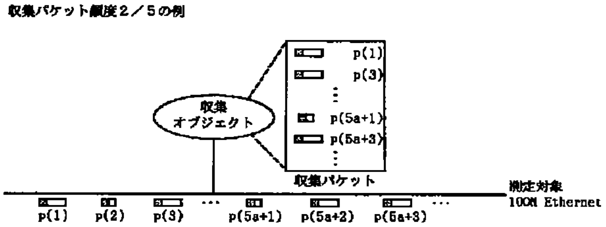
【図２】



【図３】



【図４】



フロントページの続き

(72)発明者　小松原　重之
東京都新宿区西新宿三丁目19番２号　日本
電信電話株式会社内